Diario di lavoro

|  |  |
| --- | --- |
| Luogo | Canobbio |
| Data | 27.09.2019 |

|  |
| --- |
| Lavori svolti |
| 13h15 – 13h40  Ho creato la guida per la vulnerabilità Cross-site Scripting (XSS).    Figura 1 Articolo XSS  13h40 – 14h05  Ho implementato una vulnerabilità di tipo Failure to Restrict URL Access e creato un articolo all’interno del blog che spiega come sfruttare la vulnerabilità.    Figura 2 Articolo Failure to Restrict URL Access  14h05 – 14h20  Implementata una vulnerabilità di tipo Security Misconfiguration, inoltre ho creato anche il relativo articolo all’interno del sito web che la documenta.    Figura 3 Articolo Security Misconfiguration  14h20 – 14h45  Ho creato un utente dedicato al sito web per prevenire che attraverso vulnerabilità si possano toccare anche altri database esterni.  15h00 – 16h20  Ho iniziato a pensare a come implementare la vulnerabilità SQL Injection in un modo che non sia distruttiva. Al momento è stata implementata all’interno della funzionalità di ricerca di HackerLab.  I problemi che può causare al momento sono:   * Update, Insert, Delete, Select e Drop del database hackerlab * Possibilità di eliminare file   Il problema che devo risolvere è la possibilità di eliminare file. Al momento se un utente modifica tramite SQL Injection l’immagine di un articolo può eliminare qualsiasi file a sua scelta, esempio:  a%'; UPDATE articles SET image = "../composer.json"; --  Questo perché la funzione di delete è implementata nel seguente modo:  unlink(\_\_DIR\_\_.'/../../storage/'.$article["image"]);  Quindi, ho intenzione di rendere sicura la rimozione del file in modo di permettere solamente azioni al database.  16h20 – 16h30  Stesura diario. |

|  |
| --- |
| Problemi riscontrati e soluzioni adottate |
| Non ho riscontrato nessun problema. |

|  |
| --- |
| Punto della situazione rispetto alla pianificazione |
| Mi trovo molto avanti rispetto alla pianficia. |

|  |
| --- |
| Programma di massima per la prossima giornata di lavoro |
| Rendere sicura eliminazione di file, implementare la funzionalità di reset dei dati e del database. |